6712-01

This document is scheduled to be published in the Federal Register on 10/15/2021 and available online at **federalregister.gov/d/2021-22099**, and on **govinfo.gov**

FEDERAL COMMUNICATIONS COMMISSION

47 CFR Parts 52 and 64

[WC Docket No. 21-341; FCC 21-102; FR ID 52298]

SIM Swapping and Port-Out Fraud

AGENCY: Federal Communications Commission.

ACTION: Proposed rule.

SUMMARY: In this document, the Commission adopted a Notice of Proposed Rulemaking (NPRM) that focuses on putting an end to two methods used by bad actors to take control of consumers' cell phone accounts and wreak havoc on people's financial and digital lives without ever gaining physical control of a consumer's phone. In the first type of scam, known as "subscriber identity module swapping" or "SIM swapping," a bad actor convinces a victim's wireless carrier to transfer the victim's service from the victim's cell phone to a cell phone in the bad actor's possession. In the second method, known as "port-out fraud," the bad actor, posing as the victim, opens an account with a carrier other than the victim's current carrier. The bad actor then arranges for the victim's phone number to be transferred to (or "ported out") to the account with the new carrier controlled by the bad actor. This NPRM takes aim at these scams by proposing to amend the Federal Communications Commission's (Commission) Customer Proprietary Network Information (CPNI) and local number portability (LNP) rules to require carriers to adopt secure methods of authenticating a customer before redirecting a customer's phone number to a new device or carrier. The NPRM also proposes to require providers to immediately notify customers whenever a SIM change or port request is made on customers' accounts, and seeks comment on other ways to protect consumers from SIM swapping and port-out fraud.

DATES: Comments are due on or before **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**, and reply comments are due on or before

[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. Written comments on the Paperwork Reduction Act proposed information collection requirements must be submitted by the public and other interested parties on or before **[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].**

ADDRESSES: You may send comments, identified by WC Docket No. 21-341 by any of the following methods:

- *Electronic Filers*: Comments may be filed electronically using the Internet by accessing ECFS: https://www.fcc.gov/ecfs/.
- *Paper Filers*: Parties who choose to file by paper must file an original and one copy of each filing.

  Filings can be sent by commercial overnight courier, or by first-class or overnight U.S. Postal Service mail. All filings must be addressed to the Commission's Secretary, Office of the Secretary, Federal Communications Commission.

  - Commercial overnight mail (other than U.S. Postal Service Express Mail and Priority Mail) must be sent to 9050 Junction Drive, Annapolis Junction, MD 20701.
  - U.S. Postal Service first-class, Express, and Priority mail must be addressed to 45 L Street, NE, Washington DC 20554.
- Effective March 19, 2020, and until further notice, the Commission no longer accepts any hand or messenger delivered filings. This is a temporary measure taken to help protect the health and safety of individuals, and to mitigate the transmission of COVID-19. *See* FCC Announces Closure of FCC Headquarters Open Window and Change in Hand-Delivery Policy, Public Notice, 35 FCC Rcd 2788 (2020). https://www.fcc.gov/document/fcc-closes-headquarters-open-window-and-changes-hand-delivery-policy.

People with Disabilities: To request materials in accessible formats for people with disabilities (braille, large print, electronic files, audio format), send an e-mail to fcc504@fcc.gov or call the Consumer & Governmental Affairs Bureau at (202) 418-0530 (voice), 202-418-0432 (TTY).

FOR FURTHER INFORMATION CONTACT: Wireline Competition Bureau, Competition Policy Division, Melissa Kirkel, at (202) 418-7958, Melissa.Kirkel@fcc.gov. For additional information concerning the Paperwork Reduction Act information collection requirements contained in this document, send an email to PRA@fcc.gov or contact Nicole Ongele, Nicole.Ongele@fcc.gov.

SUPPLEMENTARY INFORMATION: This is a summary of the Commission's Notice of Proposed Rulemaking (NPRM) in WC Docket No. 21-341, adopted and released on September 30, 2021. The full text of the document is available on the Commission's website at https://www.fcc.gov/document/fcc-proposes-rules-prevent-sim-swapping-and-port-out-fraud. To request materials in accessible formats for people with disabilities (e.g. braille, large print, electronic files, audio format, etc.), send an email to FCC504@fcc.gov or call the Consumer & Governmental Affairs Bureau at (202) 418-0530 (voice) or (202) 418-0432 (TTY).

Initial Paperwork Reduction Act of 1995 Analysis

This document contains proposed information collection requirements. The Commission, as part of its continuing effort to reduce paperwork burdens, invites the general public to comment on the information collection requirements contained in this document, as required by the Paperwork Reduction Act of 1995, Public Law 104-13. Public and agency comments are due **[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].**

Comments should address: (a) whether the proposed collection of information is necessary for the proper performance of the functions of the Commission, including whether the information shall have practical utility; (b) the accuracy of the Commission's burden estimates; (c) ways to enhance the quality, utility, and clarity of the information collected; (d) ways to minimize the

burden of the collection of information on the respondents, including the use of automated collection techniques or other forms of information technology; and (e) way to further reduce the information collection burden on small business concerns with fewer than 25 employees. In addition, pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107-198, *see* 44 U.S.C. 3506(c)(4), we seek specific comment on how we might further reduce the information collection burden for small business concerns with fewer than 25 employees.

Synopsis

I. NOTICE OF PROPOSED RULEMAKING

1. We believe that our CPNI and number porting rules are ripe for updates that could help prevent SIM swapping and port-out fraud. In this NPRM, we propose to prohibit wireless carriers from effectuating a SIM swap unless the carrier uses a secure method of authenticating its customer. We also propose to amend our CPNI rules to require wireless carriers to develop procedures for responding to failed authentication attempts and to notify customers immediately of any requests for SIM changes. We also seek comment on whether we should impose customer service, training, and transparency requirements specifically focused on preventing SIM swap fraud. We likewise propose to amend our number porting rules to combat port-out fraud while continuing to encourage robust competition through efficient number porting. Finally, we consider whether we should adopt any other changes to our rules to address SIM swap and port-out fraud, including the difficulties encountered by victims of these schemes. We seek comment on our proposals and invite input from stakeholders on how to best tailor the rules to combat this growing, pernicious fraudulent activity.

A. Strengthening the Commission's CPNI Rules to Protect Consumers

2. *Customer Authentication Requirements for SIM Change Requests*. To reduce the incidence of SIM swap fraud, we propose to prohibit carriers from effectuating a SIM swap unless the carrier uses a secure method of authenticating its customer, and to define "SIM" for purposes of these rules as a physical or virtual card contained with a device that stores unique information that can be identified to a specific mobile network. As used in our proposed rules, the term "carrier" includes "any officer, agent, or other person acting for or employed by any

common carrier or user, acting within the scope of his employment." We seek comment on these proposals. Consistent with the recommendations made last year by the Princeton Research team that studied SIM swapping, we propose that use of a pre-established password; a one-time passcode sent via text message to the account phone number or a pre-registered backup number; a one-time passcode sent via e-mail to the e-mail address associated with the account; or a passcode sent using a voice call to the account phone number or a preregistered back-up telephone number would each constitute a secure method of authenticating a customer prior to a SIM change. We seek comment on this proposal and whether it will serve as an effective deterrent to SIM swapping fraud. As used here, a "pre-established password" is a password chosen by the customer for future use to authenticate a customer for access to account information or to make account changes.

3. Are each of these authentication methods secure? Since 2016, the National Institute of Standards and Technology (NIST) has recognized known risks associated with SMS-based authentication, distinguishing "SMS-based authentication from other out-of-band authentications methods due to heightened security risks including 'SIM change.'" In addition, recent media reports call into question the security of using text messages for authentication purposes. For example, a recent investigation found that SMS-based text messages could be easily intercepted and re-routed using a low-cost, online marketing service that helps businesses do SMS marketing and mass messaging. As with SIM swap fraud, once the hacker was able to re-route a target's text messages, the hacker was also able to access other accounts associated with that phone number. Wireless carriers reportedly have mitigated the security vulnerability uncovered in this investigation. Has this vulnerability has been fixed so that it is no longer a threat to customers of any carrier? What rules could we adopt to ensure that authentication using text messages is secure and effective to protect consumers from SIM swap fraud? Or alternatively, should we prohibit carriers from using text messaging, or specifically SMS text messaging, to authenticate customers requesting SIM swaps? What steps could we take to

prevent a customer's text messages from being forwarded without authorization? Should we, for example, require companies offering the text forwarding services to call the customer whose texts will be forwarded to confirm consent prior to forwarding? If so, what authority may we rely upon to adopt such a rule? Are such methods effective? What other steps should we take to help secure customers' accounts and text messages?

4. All of the methods of authentication that we propose to include in the requirement to authenticate a wireless customer before allowing for a SIM swap are familiar ones, already used by consumers and companies in various other circumstances. Based on stakeholder experience with these methods of authentication, how burdensome would our proposed authentication requirement be on customers making legitimate SIM change requests? Would they pose particular challenges to customers whose phone associated with their account has been lost, stolen, or destroyed, or customers who are not comfortable with technology, or to customers with disabilities? Should customers be able to opt-in or opt-out of certain methods of authentication?

5. We also invite comment on whether there are other secure methods of authentication that we should allow carriers to use to authenticate their customers in advance of effectuating a SIM change. What practices and safeguards do carriers currently employ to authenticate customers when SIM change requests are made? Have carriers implemented any processes and protections to address SIM swap fraud specifically? If so, have those practices been effective? Do carriers use multi-factor authentication and has it been effective in preventing SIM swap fraud? If so, should we adopt a multi-factor authentication requirement to prevent SIM swap fraud? If we do require multi-factor authentication, is texting sufficiently secure to permit it as an authentication method for use in multi-factor authentication? Are there emerging technologies or authentication methods in development that could potentially be implemented to protect customers from SIM swap fraud? Are there other security measures incorporated into handsets or operating systems that can be used to authenticate or otherwise

prevent SIM swap fraud? Could blockchain technologies that store data in a decentralized manner offer additional security when authenticating customers requesting SIM changes? Are there limitations in these technologies, such as security, storage, scalability, and cost that could place a burden on providers and manufacturers of SIMs? What privacy risks are associated with any of these methods or others suggested by commenters? How effective would any of these methods be at deterring SIM swap fraud? As with the methods we have proposed, what challenges do other secure methods of authentication pose to customers and how burdensome would they be on customers making legitimate SIM change requests, particularly those customers who are no longer in possession of their cell phone because it was lost, stolen, or destroyed, or customers who are not comfortable with technology, or customers with disabilities? What are the costs to carriers for any alternative secure authentication methods?

6. If we adopt a specific set of authentication practices that carriers must employ before effectuating a SIM change, how can we account for changes in technology, recognizing that some of these methods may become hackable over time, while additional secure methods of authentication will likely be developed over time? We seek comment on whether instead of requiring specific methods of authentication, we should adopt a flexible standard requiring heightened authentication measures for SIM swap requests. The Commission has previously found that "techniques for fraud vary and tend to become more sophisticated over time" and that carriers "need leeway to engage emerging threats." The Commission has allowed carriers to determine which specific measures will best enable them to ensure compliance with the requirement that carriers take reasonable measures to discover and protect against fraudulent activity. We observe that to the extent carriers have already implemented or are considering implementing additional protections against SIM swap fraud, we want to ensure that any rules we adopt do not inhibit carriers from using and developing creative and technical solutions to prevent SIM swap fraud or impose unnecessary costs. Would codifying a limited set of methods for authenticating customers in advance of approving SIM swapping requests reduce carriers'

flexibility to design effective measures and, in effect, reduce their ability to take aggressive actions to detect and prevent fraudulent practices as they evolve? Could requiring specific methods of authentication provide a "roadmap" to bad actors? What costs would such requirements impose on carriers, particularly smaller carriers?

7. To that end, we seek comment whether we should instead require carriers to comply with the NIST Digital Identity Guidelines, which are updated in response to changes in technology, in lieu of other proposals. The NIST Digital Identity Guidelines are a set of guidelines that provide technical requirements for federal agencies "implementing digital identity services," focusing on authentication. Would requiring carriers to adopt and comply with these guidelines "future proof" authentication methods? Would these guidelines effectively protect consumers in the context of SIM swap fraud? Are these guidelines generally applicable in the telecommunications context, and do the guidelines provide sufficient flexibility to carriers? Would requiring carriers to comply with the guidelines pose any difficulties for smaller providers, and would the authentication methods recommended in the guidelines pose any particular challenges to customers? We also seek comment on whether there are other definitive government sources that we could consider adopting as appropriate authentication methods.

8. We also seek comment on what would be an appropriate implementation period for wireless carriers to implement any changes to their customer authentication processes. Because of the serious harms associated with SIM swap fraud, we believe that a speedy implementation is appropriate. Are there any barriers to a short implementation timeline and, if so, what are they? What could we do to eliminate or reduce potential obstacles? Will smaller wireless carriers need additional time to implement the requirements we propose?

9. Are there other ways we can strengthen the Commission's customer authentication rules to better protect customers from SIM swap fraud? For example, for online access to CPNI, our rules require a carrier to authenticate a customer "without the use of readily available biographical information[] or account information." Given evidence of the ease with

which bad actors can create recent payment or call detail information, we propose to make clear that carriers cannot rely on such information to authenticate customers for online access to CPNI. We invite comment on that proposal.

10. We also seek comment on whether there are other methods of authentication that carriers should be allowed to implement to prevent SIM fraud that originates in retail locations. Our rules currently allow carriers to disclose CPNI to a customer at a carrier's retail location if the customer presents a valid photo ID. We seek comment on whether a government-issued ID alone is sufficient for in-person authentication. How prevalent is in-person fraud using fake IDs as a source of SIM swap fraud? What role can, and should, retail stores play in authentication, particularly in situations where customers do not have access to technology or are not tech savvy? Should customer authentication requirements be the same for SIM changes initiated by telephone, online, or in store?

11. We also invite comment on whether we should amend our rule on passwords and back-up authentication methods for lost or forgotten passwords. Our rules require a carrier to authenticate the customer without the use of readily available biographical information or account information to establish the password. We permit carriers to create a back-up customer authentication method in the event of a lost or forgotten password, but such back-up customer authentication method may not prompt the customer for readily available biographical information or account information. Should we make changes to this requirement? If so, what changes are needed? Do the existing rules create vulnerabilities that should be addressed? Should these requirements be updated to reflect any changes in technology? How would they enhance the protections already provided to consumer passwords?

12. *Response to Failed Authentication Attempts.* We propose to require wireless carriers to develop procedures for responding to failed authentication attempts, and we seek comment on this proposal. We seek comment on what processes carriers can implement to prevent bad actors from attempting multiple authentication methods while at the same time

ensuring that protections do not negatively impact legitimate customer requests. For example, would a requirement that SIM swaps be delayed for 24 hours in the case of multiple failed authentication attempts while notifying the customer via text message and/or e-mail, be effective at protecting customers from fraudulent SIM swaps? If we adopt such a rule, should we specify the number of attempts, and if so, how many attempts should trigger the 24-hour delay? How burdensome would this be for customers, and what costs would this impose on carriers? How long would it take carriers to develop and implement procedures for responding to failed authentication attempts? Would such a requirement have anti-competitive effects?

13. *Customer Notification of SIM Change Requests.* As part of our effort to protect consumers from fraudulent SIM swapping, we propose to require wireless providers to notify customers immediately of any requests for SIM changes. We seek comment on this proposal. Is it unnecessary if we adopt specific heightened authentication requirements prior to providing a SIM swap? Or will it provide a worthwhile second line of protection against fraudulent SIM swaps?

14. Our CPNI rules currently require carriers to notify customers immediately whenever a password, customer response to a back-up means of authentication for lost or forgotten passwords, online account, or address of record is created or changed. This notification may be through a carrier-originated voicemail or text message to the telephone number of record, or by mail to the address of record, and must not reveal the changed information or be sent to the new account information. As the Commission found with respect to these other types of account changes, we believe that notification of SIM change requests could be an important tool for customers to monitor their account's security, and could help protect customers from bad actors "that might otherwise manage to circumvent []authentication protections" and enable customers "to take appropriate action in the event" of fraudulent activity. Do commenters agree?

15. We also seek comment on how this notification should be provided to customers.

We believe that the verification methods provided in our rules for other types of account changes may be insufficient to protect customers from SIM swap fraud because in these situations, the bad actor has taken control of the customer's account and any verification communications sent after the transfer by voicemail or text may be directed to the bad actor rather than to the victim. Moreover, mail to the address of record will likely be too slow to stop the ongoing fraud that may involve financial accounts, social media profiles, and other services. We therefore propose to amend our rules to include notification requirements that would more effectively alert customers to SIM fraud on their accounts and seek comment on what types of notification would be most effective in alerting customers to SIM swap fraud in progress. Would e-mail notification be more effective? Should we retain the option to send such notifications by mail even though this method involves significant delay? Should carriers be required to give customers the option of listing a personal contact (e.g., a spouse or family member) and then inform that contact that the customer is requesting a SIM swap? What other methods of communication could be used to get timely notification to customers, particularly those customers who are no longer in possession of their device because it has been lost or stolen?

16. In addition to immediate customer notification of requests for SIM swaps, we seek comment on requiring up to a 24-hour delay (or other period of time) for SIM swap requests while notifying the customer via text message, e-mail, through the carrier's app, or other push notification and requesting verification of the request. Once a customer verifies the SIM change request either via text, the carrier's app (if the device is in the customer's possession), an e-mail response, or the customer's online account, the carrier would be free to process the SIM change. If we adopt heightened authentication requirements, is a temporary delay in transferring the account to a new SIM necessary to ensure sufficient time for a customer to receive the notification of activity on the account and take action if the customer has not initiated the changes? Would this requirement be effective in preventing SIM swap fraud? How burdensome would such a delay be for customers? Are there safety implications for customers who

legitimately need a new SIM? Could such a delay prevent the customer from completing 911 calls during the waiting period? What costs would this requirement impose on carriers, and how long would it take carriers to develop, test, and implement such a process? Would such a requirement be anti-competitive? Should we consider other approaches to customer notifications of SIM transfers?

17. *Customer Service, Training, and Transparency.* Additionally, we seek comment on whether we should impose customer service, training, and/or transparency requirements specifically focused on preventing SIM swap fraud. For example, should we require carriers to modify customer record systems so that customer service representatives are unable to access CPNI until after the customer has been properly authenticated? Would this approach be effective in preventing customer service representatives from assisting with authentication through the use of leading questions or other more nefarious employee involvement in SIM swap fraud? Would a requirement for record-keeping of the authentication method used for each customer deter employee involvement in SIM swapping fraud? Are there ways to avoid employee malfeasance, such as requiring two employees to sign off on every SIM change? What burdens would be associated with these possible requirements? Anecdotal evidence suggests that, in some cases, customer service representatives are not trained on procedures to deal with customers who have been victims of SIM swap fraud, and as a result, customers who are already victims have difficulty getting help from their carriers. To address this concern, we seek comment on whether we should impose training requirements for customer service representatives to address SIM swap fraud attempts, complaints, and remediation. What costs would these measures impose on carriers? Is there a way to reduce the burdens of these proposals while still achieving the policy aims? Would these proposals reduce SIM swap fraud or otherwise impact the customer experience? How long would it take wireless carriers to implement any new training requirements? Are there alternative approaches that might be more effective or efficient?

18. We also seek comment on whether we should require wireless providers to offer

customers the option to disable SIM changes requested by telephone and/or online access (i.e., account freezes or locks). We believe that offering these protections would impose minimal burdens on carriers while offering significant protection to customers. Do commenters agree? Whether or not we require wireless providers to offer such services, we also seek comment on whether we should require carriers to provide a transparent, easy-to-understand, yearly notice to customers of the availability of any account protection mechanisms the carrier offers (e.g., SIM transfer freeze, port request freezes, PINs, etc.). What costs would such notification requirements impose on carriers? We believe that any customer notifications should be brief, use easy-to-understand language, and be delivered in a manner that is least burdensome to customers. We seek comment on what form such notifications could take and how they could be delivered to customers to provide meaningful notice of such services while imposing minimal burden on carriers. Do we need to prescribe a method or methods for customers to unfreeze or unlock their accounts? What methods would be sufficiently secure? Would an unfreeze or unlock be immediate or should there be a waiting period before an unlocked account can be transferred?

19. *Accounts with Multiple Lines.* We seek comment on how these proposed CPNI rule changes impact wireless accounts with multiple lines, such as shared or family accounts. If we require the customer to provide a one-time passcode for the carrier to execute a SIM change, should each line on the shared or family account have its own passcode? If the account owner elects to freeze the account to protect against unauthorized changes, how can we ensure that another member of the shared or family account remains able to port-out his or her number? Should the freeze option apply only to individual lines and not to entire accounts? Do our proposed rules impact these types of accounts with multiple lines in any other ways?

20. *Remediation of SIM Swap Fraud.* We seek comment on how we can enable timely resolution of SIM swap fraud to minimize financial and other damage to customers who are victims of SIM swap fraud. How can we encourage and/or ensure that carriers quickly

resolve complaints in cases of SIM swap fraud? Should we require carriers to respond to customers and offer redress within a certain time frame? What would be the costs to carriers, and what are the costs to customers if we do not do so? We seek comment on the methods wireless carriers have established to help victims of SIM swap fraud halt an unauthorized SIM swap request or to recover their phone numbers from bad actors.

21. *Carriers' Duty to Protect CPNI.* We also seek comment on codifying the Commission's expectation that carriers must take affirmative measures to discover and protect against fraudulent activity beyond the measures specifically dictated by our rules and that additional measures (e.g., self-monitoring) are required to comply with section 222's mandate to protect the confidentiality of customer information. In the *2007 CPNI Order*, the Commission codified the requirement that carriers take reasonable measures to discover and protect against unauthorized access to CPNI, and specified that adoption of the rules in that *Order* does not relieve carriers of their fundamental statutory duty to remain vigilant in their protection of CPNI, nor does it insulate them from enforcement action for unauthorized disclosure of CPNI. The Commission allowed carriers flexibility in how they would satisfy their statutory obligations but expressed an expectation that carriers would take affirmative measures to discover and protect against fraudulent activities beyond what is expressly required by the Commission's rules. We seek comment on whether codifying a requirement to take affirmative measures to discover and protect against fraudulent activities would lead to more effective measures to detect and prevent SIM swap fraud. Has the expectation expressed in 2007 been effective? Would the additional threat of enforcement of a codified rule create additional incentives for carriers to take more aggressive action to detect and prevent fraudulent access to CPNI? We seek comment on whether there are additional requirements needed to ensure that carriers comply with their legal obligations under section 222 to detect and prevent SIM swap fraud.

22. *Tracking the Effectiveness of Authentication Measures.* We seek comment on what data carriers collect about SIM swap fraud, and whether we should require that carriers

track data regarding SIM swap complaints to measure the effectiveness of their customer authentication and account protection measures. What would be the burdens of requiring wireless carriers to internally track customer SIM swap complaints? Do wireless carriers already report this information to the U.S. Secret Service and Federal Bureau of Investigation (FBI) pursuant to the Commission's rules? We also seek comment on whether we should modify our breach reporting rules to require wireless carriers to report SIM swap and port-out fraud to the Commission, and what the costs would be to carriers of doing so, including the timeframe for implementing such a requirement. Should we require carriers to inform the Commission of the authentication measures that they have in place and when those measures change? Would requiring carriers to update the Commission about changes to authentication measures, along with the frequency of customer SIM swap complaints, be sufficient to enable the Commission to evaluate the efficacy of a carrier's authentication measures, or should the Commission require carriers to provide additional information? We also seek comment on how we should ensure carrier compliance with any proposed obligations that we adopt. For example, should we specifically direct the Commission's Enforcement Bureau, or another Bureau or Office, to conduct compliance audits? Are there other audits or models that we should use as guidelines to ensure compliance? We seek comment on the best method to enforce our proposals.

23. *Applicability of Customer Authentication Measures.* We seek comment on whether any new or revised customer authentication measures we adopt should apply only to wireless carriers and only with respect to SIM swap requests, or whether such expanded authentication requirements would offer benefits for all purposes and with respect to all providers covered by our CPNI rules. Is there anything unique about VoLTE service or the upcoming Voice over New Radio (VoNR) that we need to consider? Further, as the nation's networks migrate from 2G and 3G to 4G and 5G, are there particular technical features that should be taken into consideration regarding authentication requirements? Is the type of phone number takeover that occurs through SIM swap fraud only relevant to mobile phone numbers

(due to SIM swaps and text message-based text authentication)? Are there also concerns with respect to account takeovers of interconnected Voice over Internet Protocol (VoIP) services, one-way VoIP services, and landline telephone services? Even if the same concerns are not present (or as strongly present), should we apply any stronger authentication requirements to all providers to protect customers' privacy and to provide uniform rules across all providers? If so, under what legal authority could we extend the proposed authentication requirements to services other than wireless? Is there value to uniformity with other categories of providers? Would costs imposed on these carriers outweigh the limited benefit of these requirements related to non-wireless carriers? Are there any other rules that would need to be aligned for consistency if we make changes to the CPNI rules to address SIM swap fraud? In addition, if limited to wireless providers only, we believe that any new rules we adopt should apply to all providers of wireless services, including resellers. Do commenters agree?

24. We also seek comment on whether any new rules should apply only to certain wireless services, such as pre-paid services. Is SIM swap fraud limited to, or more prevalent with, pre-paid or post-paid wireless accounts? Do wireless resellers (many of which offer pre-paid services) encounter this type of fraud more or less often than facilities-based carriers? We invite comment on whether some or all changes discussed here should apply to all mobile accounts or whether certain changes should be limited to pre-paid or post-paid accounts only. We note that pre-paid plans generally do not require credit checks and therefore subscribers to prepaid plans may be more low-income and economically vulnerable individuals. Would such requirements impose disproportionate burdens on these customers?

25. We also seek comment on the scope of any changes that we may make to the CPNI rules to address SIM swap fraud. Specifically, should any new rules be narrowly tailored to deal only with SIM swap fraud, or should they be broader to ensure that they cover the evolving state of fraud on wireless customers? Outside of the account takeover context, are there benefits to providing expanded authentication requirements before providing access to CPNI to

someone claiming to be a carrier's customer? We seek comment on whether any heightened authentication measures required (or prohibited) should apply for access to all CPNI, or only in cases where SIM change requests are being made.

26. In addition, we seek comment on the impact that our proposed rules could have on smaller carriers. Would the proposed requirements impose additional burdens on smaller carriers? Would they face different costs than larger carriers in implementing the new requirements, if adopted? Would smaller carriers need more time to comply with new authentication rules? Do they face other obstacles that we have not considered here?

27. We believe that we have authority to adopt the proposed rules discussed in this section pursuant to our authority under sections 4, 201, 222, 303, and 332 of the Act, and we seek comment on this conclusion. Do we have additional sources of authority on which we may rely here? To the extent that we have not already done so, we also solicit input on the relative costs and benefits of our proposals to amend the CPNI rules to address SIM swap fraud. How many legitimate SIM swap requests do carriers receive yearly, and what are customers' most common reasons for requesting a legitimate SIM swap? Is there any evidence concerning the degree to which authentication measures limit legitimate SIM swaps, or the degree to which they successfully prevent fraud? We ask commenters for input on how any of these proposals could positively or negatively affect the customer experience and whether they foresee any unintended consequences from the changes we propose here.

B. Strengthening the Commission's Number Porting Rules to Protect Consumers

28. We next seek comment on proposals to strengthen our number porting rules to protect customers from unauthorized ports and port-out fraud. One reason that number porting can be used to subvert two-factor authentication may be the relative ease with which carriers fulfill port order requests from other carriers. We note that though the Act makes it unlawful for any telecommunications carrier to "submit or execute a change in a subscriber's selection of a

provider of telephone exchange service . . . except in accordance with such verification procedures as the Commission shall prescribe," the Commission's slamming rules implementing this provision do not currently apply to wireless carriers. As a result, wireless subscribers are not afforded the same protections as wireline customers when their service is switched to another carrier without their authorization. The Commission has, in the past, been concerned that adding "additional steps for the customer would also add a layer of frustration and complexity to the number porting process, with anticompetitive effects." While the Commission remains committed to "facilitat[ing] greater competition among telephony providers by allowing customers to respond to price and service changes . . . ," we seek comment below on what additional measures we can adopt to protect customers from port-out fraud.

29. *Notification of Wireless Port Requests and Customer Authentication Processes.* We propose to require wireless carriers to provide notification to customers through text message or other push notification to the customer's device whenever a port-out request is made to ensure that customers may take action in the event of an unauthorized port request, and seek comment on our proposal. For example, Verizon sends its customers a text message letting the customer know that a port-out request has been initiated. When the request is completed, Verizon will send the customer an e-mail stating that the port to the new service was successful. AT&T may also "send customers a text message to help protect them from illegal porting. This notification will not prevent or delay the customer's request. It just adds a simple step to better protect against fraud." We believe that requiring customer notice of port requests could be a minimally intrusive protective measure that could be automated to minimize delays while providing significant protections for customers. Do commenters agree? Do other carriers currently notify their customers of port-out requests? What would be the costs for carriers to implement such a requirement, particularly for smaller carriers? How much time would carriers need to implement such a requirement? Would requiring notification of port requests to customers harm competition? Is there a particular method of notification that is most effective? For this and

other potential rules that may require text messages and/or push notifications, should we define the scope of permissible text messages or other push notifications and, if so, what definition or definitions should we use?

30. We also seek comment on whether a port request notification requirement is sufficient to protect customers from port-out fraud, or whether we should also require customer verification or acknowledgement of the text message or push notification through a simple Yes/No response mechanism. Would a customer port verification requirement unreasonably hinder the porting process, and could it be used anticompetitively by carriers? Should we require that customers respond within a certain amount of time before the carrier can execute the port? We recognize that some customers may not frequently check their text messages or push notifications, which could lead to a delay if we require the customer to verify the port. Should we require carriers to send follow-up messages to the customer via e-mail or a phone call? What other processes have wireless carriers adopted to protect customers from port-out fraud, and have they been effective in reducing port-out fraud?

31. As discussed above, the National Institute of Standards and Technology and recent media reports call into question the security of using text messages for authentication purposes. Is notification and/or verification of a port request via text message a secure means of authenticating the validity of a customer's wireless port request? Should we instead require an automated notification call and verification response through a voice call or other method, such as e-mail or carrier app? What methods would ensure that customers who have voice-and-text-only service, or whose devices are incapable of accessing a carrier's app or website, are not hindered in their porting choices? Are there any barriers for smaller carriers implementing any of these changes to protect customers' accounts from port-out fraud?

32. We seek comment whether we should require customers' existing wireless carriers to authenticate a customer's wireless port request through means other than the fields used to validate simple port requests. Are the benefits of potentially protecting customers from

port-out fraud outweighed by the potential harms to competition from delaying or impeding customers' valid wireless number port requests? We seek comment on the processes that wireless carriers, including MVNO providers, resellers, and smaller carriers, currently use to authenticate customer port-out requests, and whether those methods are effective in preventing port-out fraud. According to CTIA, "[w]ireless providers are constantly improving internal processes to stay ahead of . . . bad actors, while protecting the rights of legitimate customers to transfer their phone number to a new device or wireless provider," including "[s]ending one-time passcodes via text message or e-mail to the account phone number or the e-mail associated with the account when changes are requested . . . ." Verizon will not allow its customers to transfer their number to a different carrier unless that customer first requests a Number Transfer Pin. When a Verizon customer requests a port from its new service provider, the customer must present the Verizon account number and Number Transfer Pin in order to authenticate the request. AT&T customers can create a unique passcode that in most cases the customer is required to provide "before any significant changes can be made including porting through another carrier," and starting September 30, 2021, will require customers to request a Number Transfer PIN to transfer their number to another service provider, which will replace the account passcode customers currently use. T-Mobile assigns each of its customer accounts a 6-15 digit PIN that must be provided whenever an individual requests to port-out the phone number associated with that account. Have such port-out PINs been effective at protecting customers from port-out fraud? Have carriers noticed any effect from adopting port-out PINs or other additional security measures on their customers' likelihood of switching carriers? Is there any evidence indicating how security measures affect porting frequency? Should we require wireless carriers to authenticate customers for wireless port requests under the same standard as we require carriers to authenticate customers for SIM change requests, recognizing that in the porting context, the Act sets forth competing goals of protecting customer information and promoting competition through local number porting? What would be the benefits and costs of

doing so?

33. We seek comment on any other technical or innovative solutions for customer authentication for port requests that carriers could implement to reduce port-out fraud. For example, are there technologies developed out of the Mobile Authentication task force, a collaboration among the three major U.S. wireless carriers, that could be easily implemented into the port authentication process? ZenKey, which was developed under the auspices of the Mobile Authentication task force, "collects and shares device and account data with your wireless carrier . . . [to] easily and more securely authenticate, sign up, and sign in," and "uses multi-factor authentication, including unique network signals, to not only verify a user's device but also allow verification that the user is who they say they are." Could carriers use similar technology to authenticate wireless customer port requests? What would be the costs of doing so and what are the challenges to implementation, including customer privacy and consent implications? What other technologies exist that carriers could use to quickly and effectively authenticate wireless port requests to reduce port-out fraud? As the nation's networks migrate from 2G and 3G to 4G and 5G, are there particular technical features that should be taken into consideration for protecting customers from port-out fraud?

34. We seek comment on whether we should require all carriers to implement any of the additional authentication processes for wireless port requests some providers have already developed and implemented. Is there value in uniformity? Would it reduce consumer confusion if we mandate the same authentication requirements on all wireless port-out requests regardless of the providers involved? Would that potential reduction in consumer confusion outweigh the benefits of enabling carriers to create innovative procedures to protect against port-out fraud attempts as they evolve? Would requiring specific additional customer authentication procedures, as opposed to simply making it clear that carriers are responsible for preventing port-out fraud, provide a roadmap to bad actors? Should we instead require carriers to develop heightened customer authentication procedures like those already initiated by the three

nationwide wireless carriers, but provide flexibility to the individual carriers to create and employ what works best for their service? Should we require different authentication procedures for pre-paid wireless account port-out requests than we do for post-paid wireless account port-out requests? We also seek comment on what implementation period the wireless industry would need to implement any additional validation requirements and processes we adopt.

35. We seek comment on how additional port authentication requirements would affect the timing of simple wireless-to-wireless ports. Would allowing additional authentication procedures cause unreasonable delay to the wireless porting process or cause harm to competition? In adopting any additional customer authentication requirements, we want to ensure that we leave carriers in a position to innovate and address new problems as they arise. Relatedly, we seek comment on whether it is necessary to codify a simple wireless-to-wireless porting interval to ensure that any new port authentication requirements do not lead to delay in the current porting process. The wireless industry has voluntarily established an industry standard of two and one-half hours for simple wireless-to-wireless ports. Should we codify this interval in our rules?

36. *Port-Freeze Offerings*. We propose to require all wireless providers, including resellers, to offer customers the option to place a "port-freeze" on their accounts at no cost to the customer to help deter port-out fraud. We observe that our rules currently permit local exchange carriers (LECs) to offer their customers the ability to "prevent[] a change in a subscriber's preferred carrier selection unless the subscriber gives the carrier from whom the freeze was requested his or her express consent." Should we require wireless providers to offer a similar option, and would making this option available to wireless customers deter wireless port-out fraud? Verizon offers customers the option to lock their number, blocking all port-out requests unless the account owner turns off the Number Lock feature through the Verizon mobile app, on Verizon's website, or by calling customer service. Do other wireless carriers currently offer a similar feature? Has this feature, and others like it, been successful at deterring port-out fraud?

What costs would offering this feature impose on carriers? How can we make sure that customers are easily notified of this feature? Would a one-time notice for existing customers, and notice at the time service is started, be effective at notifying customers? How often should carriers provide this notice to customers? What method would be least burdensome on carriers while also notifying all customers, including those that do not access their accounts through online services or carrier apps, of the availability of this feature? Local exchange carriers who offer their customers the "preferred carrier freeze" option must follow specific requirements regarding the solicitation and imposition of this option. Should we extend similar requirements to wireless carriers? If we impose these requirements, would the benefits gained by deterring port-out fraud outweigh the costs of this measure? What happens when a customer locks his or her account but is unable to recall the information necessary to unlock their account? Should there be a back-up authentication method available? Are there other methods wireless carriers use to prevent unauthorized port requests that we should consider requiring?

37. *Wireless Port Validation Fields.* We also propose to codify the types of information carriers must use to validate simple wireless-to-wireless port requests. Pursuant to the Commission's *2007 LNP Four Fields Declaratory Ruling*, the wireless industry agreed to use three fields of customer-provided information—telephone number, account number, and ZIP code—plus a passcode field (if customer-initiated) to validate requests for simple wireless-to-wireless ports. We propose to codify this requirement in our rules for simple wireless-to-wireless ports, just as we have codified field requirements for simple wireline and intermodal ports. We preliminarily believe that standardizing the fields necessary to complete a simple wireless-to-wireless port will allow for quicker and more efficient porting, and we seek comment on this view. We propose adopting the existing fields because we are cognizant that imposing new or different customer-required information fields could complicate the porting process, from both the carrier and customer perspectives, and we seek comment on this view. We seek comment whether codifying the existing fields used for validating simple wireless ports, in

combination with immediate customer notification of port-requests and the offering and advertisement of port-freeze options as we propose, would help to protect customers from port-out fraud. Do such measures appropriately balance the competitive benefits of rapid porting with protecting customers' accounts from fraud?

38. Are there additional fields of customer-provided information we should require for validation of wireless-to-wireless ports to minimize port-out fraud, while ensuring the continued rapid execution of valid port-out requests? If we require additional fields of customer-provided information for only wireless-to-wireless simple ports, will that cause unnecessary complications for the telecommunications industry as a whole? Will it impose additional costs on wireless carriers that would reduce competition in the telecommunications marketplace? We seek comment on whether requiring carriers to implement changes to the wireless port validation requirements would significantly impair the customer's ability to perform a legitimate port-out request. Would requiring carriers to implement additional customer-provided fields for wireless port requests stifle the ability of customers to switch carriers while retaining their phone number or keep customers locked into contracts with their current service providers? Would customers still be able to respond to price and service changes in a quick and efficient manner? Finally, we propose to make clear that any customer validation requirements apply to both facilities-based wireless carriers and resellers of wireless service and we seek comment on that proposal.

39. We seek comment on whether we should require carriers to implement a customer-initiated passcode field for all wireless number port requests, or whether it should remain optional. While AT&T, Verizon, and T-Mobile offer this option, it is unclear if all customers are required to participate. What would be the burden on customers and carriers, particularly smaller carriers, were we to mandate passcode fields for wireless number port requests? Could it harm competition and cause customer frustration if a customer has either not set up a passcode or does not know how to set up a passcode? Should we require carriers to make a customer-initiated passcode optional on an opt-out rather than opt-in basis? What steps

could carriers take to make it least burdensome on customers to establish an account passcode for wireless number porting purposes? We also seek comment on how we can ensure that a customer can make a legitimate port request if he forgets his passcode.

40. *Remediating Port-Out Fraud.* We seek comment on how we can ensure timely resolution of unauthorized port-out requests to minimize financial and other damage to customers who are victims of such fraud. What information do wireless carriers currently collect about port-out fraud? Are wireless carriers already tracking instances of customer complaints regarding this issue? Should we require that carriers use this information to measure the effectiveness of their customer authentication and account protection measures? How can we encourage and/or ensure that carriers coordinate and work together to quickly resolve complaints in cases of port-out fraud? Should we require carriers to respond to customers who allege they are victims of port-out fraud and to offer redress to such customers within a certain time frame? What would be the costs to carriers, and what are the costs to customers if we do not do so? We seek comment on the methods wireless carriers have established to help victims of port-out fraud stop an unauthorized port-out request or to recover their phone numbers from bad actors.

41. *Accounts with Multiple Lines.* We seek comment on how the proposed changes to our LNP rules impact wireless accounts with multiple lines, such as shared or family accounts. If we require the customer to provide a one-time passcode for the carrier to execute the port, should each line on the shared or family account have its own passcode? If the account owner elects to freeze the account to protect against unauthorized changes, how can we ensure that another member of the shared or family account remains able to port-out their number? Should the port-freeze option apply only to individual lines and not to entire accounts? Do our proposed rules impact these types of accounts with multiple lines in any other ways?

42. *Role of Administrator.* We also seek comment on whether the Local Number Portability Administrator (LNPA) can play a role in thwarting port-out fraud by serving as an authorized neutral third-party to verify customer identification prior to authorizing a port-out

request. The LNPA operates the Number Portability Administration Center (NPAC), which "is the system that supports the implementation of LNP and is used to facilitate number porting in the United States. The LNPA, through the NPAC, currently works with a customer's new service provider to create a number port and sends a notification to the old service provider, once the existing service provider validates and confirms the subscriber's information. What information regarding port requests does the NPAC retain? Is there additional information regarding port requests the NPAC should retain to help prevent port-out fraud? What records could be helpful if provided to customers who have been victims of unauthorized port-out fraud? Through what means and under what conditions, if any, should wireless providers permit their customers to access NPAC data regarding port requests that pertain to the customer's telephone number? Are there additional obligations that we should direct or encourage North American Portability Management, LLC, which oversees the LNPA contract, to impose on the LNPA to safeguard against port-out fraud?

43. As discussed above, the Number Portability Industry Forum has created "Best Practices" for porting between and within telephony carriers. Best Practice 73 (Unauthorized Port Flow) specifically addresses carrier processes for responding to unauthorized ports, including fraudulent ports, which are ports "which occurred as the result of an intentional act of fraud, theft, and/or misrepresentation." We seek comment on the extent to which wireless providers have adopted Best Practice 73. If wireless carriers have adopted Best Practice 73, is it effective in addressing port-out fraud? Are there changes we can make to the process flow to better protect customers? If wireless carriers have not implemented Best Practice 73, we seek comment on other methods they use to investigate potentially fraudulent ports and how they restore service to the customer. Should we require mobile carriers to adopt Best Practice 73 to help speed resolution of fraudulent port complaints? We also seek comment on what role the North American Numbering Council (NANC) can play in establishing updated best practices to protect customers from port-out fraud and in reaching industry consensus.

44. *Partial Porting Fraud.* We seek comment on whether the proposals on which we seek comment above would also be effective against partial porting fraud, where the bad actor changes the consumer's carrier for delivery of SMS messages without changing their primary carrier. Would our proposed customer notification and authentication rule prevent routing of SMS messages through an alternate provider without customer notification? Would a port freeze prevent changing the delivery provider and destination of SMS messages? If not, what changes to the proposed rules would be required to ensure they also apply to partial porting fraud? What additional measures would be necessary to prevent partial porting fraud in addition to the fraud that may occur when a wireless provider completely ports a consumer's mobile service?

45. *Impact on Smaller Carriers.* We seek comment on the impact the LNP rule changes that we discuss above could have on smaller carriers. Would these new requirements impose undue burdens on smaller carriers? Would smaller carriers face different costs from larger carriers in implementing the new requirements, if adopted? Would smaller carriers need more time to comply with revised number porting rules? Do they face other obstacles that we have not considered here?

46. *Legal Authority.* Finally, we seek comment on our legal authority to adopt the possible rules discussed in this section. We propose to rely on authority derived from sections 4, 201, 251(b)(2), 251(e), 303, and 332 of the Act to implement the proposed changes to our number porting rules to address port-out fraud, and seek comment on our proposal. Are there additional sources of authority on which the Commission can rely to implement these proposals? Should we extend any of the LNP rules on which we seek comment to any entities other than wireless carriers, such as landline carriers or VoIP providers? If so, we propose concluding that we have authority to do so pursuant to section 251(e), and we seek comment on this view. We also seek comment on whether we should update the references to "CMRS" in the Commission's number porting rules to reflect evolving technology. Finally, we solicit input on the relative costs and benefits of our proposals to amend the LNP rules to address port-out fraud.

C. Additional Consumer Protection Measures

47. Finally, we seek comment on any additional rules that would help protect customers from SIM swap or port-out fraud or assist them with resolving problems resulting from such incidents. We are aware that customers sometimes need documentation of the fraud incident to provide to law enforcement, financial institutions, or others to resolve financial fraud or other harms of the incident. A SIM swap or port-out fraud victim may have difficulty obtaining such documentation from the carrier because the carrier may not have processes in place to produce such documentation. To provide support for customers who have become victims, we seek comment on requiring wireless carriers to provide to customers (upon request) documentation of SIM swap or port-out fraud on accounts that the customer may then provide to law enforcement, financial institutions, or others. We seek comment on what information should be included in the documentation provided by carriers. We also seek comment on the potential benefits and projected costs of this proposal, including on smaller providers. Further, we invite input on how the proposed rule would affect the customer experience, either positively or negatively.

48. Next, we seek comment on other measures we can adopt to ensure that customers have easy access to information they need to report SIM swap, port-out, or other fraud. As discussed above, we believe that customer service representatives should be trained on how to assist customers who have been victims of SIM swap or port-out fraud, and carriers should have procedures in place for a response. Identity theft, including SIM swap fraud, can cause intense anxiety for victims and must be addressed in a timely manner to prevent financial losses and exposure of personal information. Thus, in addition to providing documentation, we believe that it should be easy for a customer to get access to appropriate carrier resources that can help mitigate the significant harms caused by SIM swap or port-out fraud. As such, we seek comment on whether we should adopt rules addressing how wireless carriers deal with customers once they have become victims of SIM swapping and port-out fraud. What procedures do carriers

have in place to assist customers in these circumstances and are these procedures effective? What additional steps can carriers take to recover the account and stop the ongoing fraudulent activity? How can carriers ensure that customers have easy access to the information they need to report SIM swap fraud? Should we require wireless carriers to establish a dedicated point or method of contact that is easily accessible by customers and is made available on the carrier's website so that customers can get timely assistance from their carriers? Or, given the time-sensitive nature of most fraud, would it make sense to require carriers to have a dedicated and publicized fraud hotline that customers can call directly in the case of suspected fraud? What costs would such a requirement impose on carriers, and how long would it take for carriers to implement? Are any of the Commission's existing rules obstacles to helping customers recover following a SIM swap or port-out fraud incident?

49. We seek comment on whether there are other customer protections we could adopt to address the problems associated with SIM swap and port-out fraud. For example, should the Commission require wireless carriers to enable "fraud alerts" on accounts and publicize these services to customers? Such fraud alerts could trigger additional protections when changes are requested on the accounts. Would such a requirement be effective at deterring SIM swap and port-out fraud? Would it have any unintended consequences for customers? What would such a requirement cost? Are there any other consumer protections that would be effective in combatting SIM swap and port-out fraud and, if so, how would they operate? What would be their relative costs and benefits? For example, we understand that in other countries, carriers and financial institutions share information about SIM transfers to limit damages to consumers resulting from incidents of SIM swap fraud. As discussed above, section 222 strictly limits carriers' ability to share a customer's CPNI without the customer's consent. Can we, and should we, encourage carriers to establish a mechanism based on express customer consent that would enable a financial institution to determine whether a SIM transfer had been recently completed to help protect customers from the financial harms of SIM swap and port-out fraud?

If so, should we require or encourage carriers to ask for customer permission upon set up of accounts (and to send out one-time notice to all existing customers asking if they want to permit this)? Should such a rule require retention of the record of this permission for some designated period of time? Should carriers be permitted to charge a fee for this service either to the wireless customer or to the financial institution? Are there other types of institutions that might need access to the same type of information to prevent fraud? Should our rules expressly permit or prohibit this type of service? What are the potential risks and benefits to consumers? We seek comment on how we can ensure that customers are able to take advantage of third-party fraud services to protect against SIM swap and port-out fraud.

50. We tentatively conclude that our broad Title III authority would support imposing additional consumer protection obligations such as those discussed in this section on wireless carriers. We also seek comment on whether authority derived from sections 4, 201, 222, 251, 303, and 332 would support such additional consumer protection measures. Should we extend any new consumer protection requirements to interconnected VoIP services, one-way VoIP services, or landline services? If so, pursuant to what legal authority would the Commission adopt such rules? We invite commenters to discuss the relative costs and benefits of these proposals and any foreseeable unintended consequences of the measures we discuss.

51. We seek comment on whether there are standards-setting bodies, industry organizations, or consumer groups that could evaluate this issue to augment our understanding and present possible solutions. For example, could the Alliance for Telecommunications Industry Solutions (ATIS) provide technical expertise that would be useful in determining the best course of action by the Commission to protect customers from SIM swap or port-out fraud? Could relevant trade associations work to develop industry consensus solutions to the problem?

52. *Digital Equity and Inclusion.* Finally, the Commission, as part of its continuing effort to advance digital equity for all, including people of color, persons with disabilities, persons who live in rural or Tribal areas, and others who are or have been historically

underserved, marginalized, or adversely affected by persistent poverty or inequality, invites comment on any equity-related considerations and benefits (if any) that may be associated with the proposals and issues discussed herein. Specifically, we seek comment on how our proposals may promote or inhibit advances in diversity, equity, inclusion, and accessibility, as well the scope of the Commission's relevant legal authority. The term "equity" is used here consistent with Executive Order 13985 as the consistent and systematic fair, just, and impartial treatment of all individuals, including individuals who belong to underserved communities that have been denied such treatment, such as Black, Latino, and Indigenous and Native American persons, Asian Americans and Pacific Islanders and other persons of color; members of religious minorities; lesbian, gay, bisexual, transgender, and queer (LGBTQ+) persons; persons with disabilities; persons who live in rural areas; and persons otherwise adversely affected by persistent poverty or inequality. *See* Exec. Order No. 13985, 86 Fed. Reg. 7009, Executive Order on Advancing Racial Equity and Support for Underserved Communities Through the Federal Government (January 20, 2021).

II. INITIAL REGULATORY FLEXIBILITY ANALYSIS

53. As required by the Regulatory Flexibility Act of 1980, as amended (RFA), the Commission has prepared this Initial Regulatory Flexibility Analysis (IRFA) of the possible significant economic impact on a substantial number of small entities by the policies and rules proposed in the Notice of Proposed Rulemaking (NPRM). Written comments are requested on this IRFA. Comments must be identified as responses to the IRFA and must be filed by the deadlines for comments on the NPRM provided on the first page of the item. The Commission will send a copy of the NPRM, including this IRFA, to the Chief Counsel for Advocacy of the Small Business Administration (SBA). In addition, the NPRM and IRFA (or summaries thereof) will be published in the Federal Register.

A. Need For, and Objectives of, the Proposed Rules

54. This item focuses developing protections to address SIM swapping and port-out

fraud. In SIM swapping, the bad actor targets a consumer's subscriber identity module (SIM) and convinces the victim's wireless carrier to transfer the victim's service from the original device (and that device's SIM) to a cell phone in the bad actor's possession. A consumer's wireless phone number is associated with the SIM in that consumer's cell phone; by "swapping" the SIM associated with a phone number, the bad actor can take control of a consumer's cell phone account. In "port-out fraud," the bad actor, posing as the victim, opens an account with a carrier other than the victim's current carrier. The bad actor then arranges for the victim's phone number to be transferred to (or "ported out") to the account with the new carrier controlled by the bad actor.

55. We have received numerous consumer complaints from people who have suffered significant distress, inconvenience, and financial harm as a result of SIM swapping and port-out fraud. Today, we take aim at these scams, with the goal of foreclosing these opportunistic ways in which bad actors take over consumers' cell phone accounts. Section 222 of the Communications Act of 1934, as amended (the "Act"), and our Customer Proprietary Network Information (CPNI) rules, which govern the use, disclosure, and protection of sensitive customer information to which a telecommunications carrier has access, require carriers to take reasonable measures to discover and protect against attempts to gain unauthorized access to customers' private information. Our Local Number Portability (LNP) rules govern the porting of telephone numbers from one carrier to another. Yet, it appears that neither our CPNI rules nor our LNP rules are adequately protecting consumers against SIM swap and port-out fraud. We, therefore, propose to amend our CPNI and LNP rules to require carriers to adopt secure methods of authenticating a customer before redirecting a customer's phone number to a new device or carrier. We also propose to require providers to immediately notify customers whenever a SIM change or port request is made on customers' accounts, and we seek comment on other ways to protect consumers from SIM swapping and port-out fraud.

B. Legal Basis

56. The legal basis for any action that may be taken pursuant to this NPRM is contained in sections 1, 4(i), 4(j), 201, 222, 251, 303(r), and 332 of the Communications Act of 1934, as amended, 47 U.S.C. sec. 151, 154, 201, 222, 251, 303(r), 332.

C. Description and Estimate of the Number of Small Entities to Which the Proposed Rules Will Apply

57. The RFA directs agencies to provide a description of, and, where feasible, an estimate of the number of small entities that may be affected by the proposed rules and policies, if adopted. The RFA generally defines the term "small entity" as having the same meaning as the terms "small business," "small organization," and "small governmental jurisdiction." In addition, the term "small business" has the same meaning as the term "small business concern" under the Small Business Act. A "small business concern" is one which: (1) is independently owned and operated; (2) is not dominant in its field of operation; and (3) satisfies any additional criteria established by the SBA.

58. *Small Businesses, Small Organizations, Small Governmental Jurisdictions*. Our actions, over time, may affect small entities that are not easily categorized at present. We therefore describe here, at the outset, three broad groups of small entities that could be directly affected herein. First, while there are industry specific size standards for small businesses that are used in the regulatory flexibility analysis, according to data from the Small Business Administration's (SBA) Office of Advocacy, in general a small business is an independent business having fewer than 500 employees. These types of small businesses represent 99.9 percent of all businesses in the United States, which translates to 30.7 million businesses.

59. Next, the type of small entity described as a "small organization" is generally "any not-for-profit enterprise which is independently owned and operated and is not dominant in its field." The Internal Revenue Service (IRS) uses a revenue benchmark of $50,000 or less to delineate its annual electronic filing requirements for small exempt organizations. Nationwide,

for tax year 2018, there were approximately 571,709 small exempt organizations in the U.S. reporting revenues of $50,000 or less according to the registration and tax data for exempt organizations available from the IRS.

60. Finally, the small entity described as a "small governmental jurisdiction" is defined generally as "governments of cities, counties, towns, townships, villages, school districts, or special districts, with a population of less than fifty thousand." U.S. Census Bureau data from the 2017 Census of Governments indicate that there were 90,075 local governmental jurisdictions consisting of general purpose governments and special purpose governments in the United States. Of this number there were 36,931 general purpose governments (county, municipal and town or township) with populations of less than 50,000 and 12,040 special purpose governments - independent school districts with enrollment populations of less than 50,000.

1. Providers of Telecommunications and Other Services

61. *Wired Telecommunications Carriers*. The U.S. Census Bureau defines this industry as "establishments primarily engaged in operating and/or providing access to transmission facilities and infrastructure that they own and/or lease for the transmission of voice, data, text, sound, and video using wired communications networks. Transmission facilities may be based on a single technology or a combination of technologies. Establishments in this industry use the wired telecommunications network facilities that they operate to provide a variety of services, such as wired telephony services, including VoIP services, wired (cable) audio and video programming distribution, and wired broadband internet services. By exception, establishments providing satellite television distribution services using facilities and infrastructure that they operate are included in this industry." The SBA has developed a small business size standard for Wired Telecommunications Carriers, which consists of all such companies having 1,500 or fewer employees. U.S. Census Bureau data for 2012 show that there were 3,117 firms that operated that year. Of this total, 3,083 operated with fewer than 1,000

employees. Thus, under this size standard, the majority of firms in this industry can be considered small.

62. *Local Exchange Carriers (LECs)*. Neither the Commission nor the SBA has developed a size standard for small businesses specifically applicable to local exchange services. The closest applicable NAICS Code category is Wired Telecommunications Carriers. Under the applicable SBA size standard, such a business is small if it has 1,500 or fewer employees. U.S. Census Bureau data for 2012 show that there were 3,117 firms that operated for the entire year. Of that total, 3,083 operated with fewer than 1,000 employees. Thus under this category and the associated size standard, the Commission estimates that the majority of local exchange carriers are small entities.

63. *Incumbent Local Exchange Carriers (LECs).* Neither the Commission nor the SBA has developed a small business size standard specifically for incumbent local exchange services. The closest applicable NAICS Code category is Wired Telecommunications Carriers. Under the applicable SBA size standard, such a business is small if it has 1,500 or fewer employees. U.S. Census Bureau data for 2012 indicate that 3,117 firms operated the entire year. Of this total, 3,083 operated with fewer than 1,000 employees. Consequently, the Commission estimates that most providers of incumbent local exchange service are small businesses that may be affected by our actions. According to Commission data, one thousand three hundred and seven (1,307) Incumbent Local Exchange Carriers reported that they were incumbent local exchange service providers. Of this total, an estimated 1,006 have 1,500 or fewer employees. Thus, using the SBA's size standard the majority of incumbent LECs can be considered small entities.

64. *Interexchange Carriers (IXCs)*. Neither the Commission nor the SBA has developed a small business size standard specifically for Interexchange Carriers. The closest applicable NAICS Code category is Wired Telecommunications Carriers. The applicable size standard under SBA rules is that such a business is small if it has 1,500 or fewer employees.

U.S. Census Bureau data for 2012 indicate that 3,117 firms operated for the entire year. Of that number, 3,083 operated with fewer than 1,000 employees. According to internally developed Commission data, 359 companies reported that their primary telecommunications service activity was the provision of interexchange services. Of this total, an estimated 317 have 1,500 or fewer employees. Consequently, the Commission estimates that the majority of interexchange service providers are small entities.

65. *Competitive Local Exchange Carriers (Competitive LECs). Competitive Access Providers (CAPs), Shared-Tenant Service Providers, and Other Local Service Providers.* Neither the Commission nor the SBA has developed a small business size standard specifically for these service providers. The appropriate NAICS Code category is Wired Telecommunications Carriers and under that size standard, such a business is small if it has 1,500 or fewer employees. U.S. Census Bureau data for 2012 indicate that 3,117 firms operated during that year. Of that number, 3,083 operated with fewer than 1,000 employees. Based on these data, the Commission concludes that the majority of Competitive LECS, CAPs, Shared-Tenant Service Providers, and Other Local Service Providers, are small entities. According to Commission data, 1,442 carriers reported that they were engaged in the provision of either competitive local exchange services or competitive access provider services. Of these 1,442 carriers, an estimated 1,256 have 1,500 or fewer employees. In addition, 17 carriers have reported that they are Shared-Tenant Service Providers, and all 17 are estimated to have 1,500 or fewer employees. Also, 72 carriers have reported that they are Other Local Service Providers. Of this total, 70 have 1,500 or fewer employees. Consequently, based on internally researched FCC data, the Commission estimates that most providers of competitive local exchange service, competitive access providers, Shared-Tenant Service Providers, and Other Local Service Providers are small entities.

66. *Local Resellers*. The SBA has not developed a small business size standard specifically for Local Resellers. The closest NAICS Code Category is Telecommunications

Resellers. The Telecommunications Resellers industry comprises establishments engaged in purchasing access and network capacity from owners and operators of telecommunications networks and reselling wired and wireless telecommunications services (except satellite) to businesses and households. Establishments in this industry resell telecommunications; they do not operate transmission facilities and infrastructure. MVNOs are included in this industry. The SBA has developed a small business size standard for the category of Telecommunications Resellers. Under that size standard, such a business is small if it has 1,500 or fewer employees. 2012 U.S. Census Bureau data show that 1,341 firms provided resale services during that year. Of that number, 1,341 operated with fewer than 1,000 employees. Thus, under this category and the associated small business size standard, the majority of these resellers can be considered small entities. According to Commission data, 881 carriers have reported that they are engaged in the provision of toll resale services. Of this total, an estimated 857 have 1,500 or fewer employees. Consequently, the Commission estimates that the majority of local resellers are small entities.

67. *Toll Resellers*. The Commission has not developed a definition for Toll Resellers. The closest NAICS Code Category is Telecommunications Resellers. The Telecommunications Resellers industry comprises establishments engaged in purchasing access and network capacity from owners and operators of telecommunications networks and reselling wired and wireless telecommunications services (except satellite) to businesses and households. Establishments in this industry resell telecommunications; they do not operate transmission facilities and infrastructure. MVNOs are included in this industry. The SBA has developed a small business size standard for the category of Telecommunications Resellers. Under that size standard, such a business is small if it has 1,500 or fewer employees. 2012 U.S. Census Bureau data show that 1,341 firms provided resale services during that year. Of that number, 1,341 operated with fewer than 1,000 employees. Thus, under this category and the associated small business size standard, the majority of these resellers can be considered small entities. According to Commission data,

881 carriers have reported that they are engaged in the provision of toll resale services. Of this total, an estimated 857 have 1,500 or fewer employees. Consequently, the Commission estimates that the majority of toll resellers are small entities.

68. *Wireless Telecommunications Carriers (except Satellite)*. This industry comprises establishments engaged in operating and maintaining switching and transmission facilities to provide communications via the airwaves. Establishments in this industry have spectrum licenses and provide services using that spectrum, such as cellular services, paging services, wireless internet access, and wireless video services. The appropriate size standard under SBA rules is that such a business is small if it has 1,500 or fewer employees. For this industry, U.S. Census Bureau data for 2012 show that there were 967 firms that operated for the entire year. Of this total, 955 firms employed fewer than 1,000 employees and 12 firms employed of 1000 employees or more. Thus under this category and the associated size standard, the Commission estimates that the majority of Wireless Telecommunications Carriers (except Satellite) are small entities.

69. The Commission's own data—available in its Universal Licensing System—indicate that, as of August 31, 2018 there are 265 Cellular licensees that will be affected by our actions. The Commission does not know how many of these licensees are small, as the Commission does not collect that information for these types of entities. Similarly, according to internally developed Commission data, 413 carriers reported that they were engaged in the provision of wireless telephony, including cellular service, Personal Communications Service (PCS), and Specialized Mobile Radio (SMR) Telephony services. Of this total, an estimated 261 have 1,500 or fewer employees, and 152 have more than 1,500 employees. Thus, using available data, we estimate that the majority of wireless firms can be considered small.

70. *Satellite Telecommunications.* This category comprises firms "primarily engaged in providing telecommunications services to other establishments in the telecommunications and broadcasting industries by forwarding and receiving communications signals via a system of

satellites or reselling satellite telecommunications." Satellite telecommunications service providers include satellite and earth station operators. The category has a small business size standard of $35 million or less in average annual receipts, under SBA rules. For this category, U.S. Census Bureau data for 2012 show that there were a total of 333 firms that operated for the entire year. Of this total, 299 firms had annual receipts of less than $25 million. Consequently, we estimate that the majority of satellite telecommunications providers are small entities.

71. *All Other Telecommunications*. The "All Other Telecommunications" category is comprised of establishments primarily engaged in providing specialized telecommunications services, such as satellite tracking, communications telemetry, and radar station operation. This industry also includes establishments primarily engaged in providing satellite terminal stations and associated facilities connected with one or more terrestrial systems and capable of transmitting telecommunications to, and receiving telecommunications from, satellite systems. Establishments providing Internet services or voice over Internet protocol (VoIP) services via client-supplied telecommunications connections are also included in this industry. The SBA has developed a small business size standard for "All Other Telecommunications," which consists of all such firms with annual receipts of $35 million or less. For this category, U.S. Census Bureau data for 2012 show that there were 1,442 firms that operated for the entire year. Of those firms, a total of 1,400 had annual receipts less than $25 million and 15 firms had annual receipts of $25 million to $49,999,999. Thus, the Commission estimates that the majority of "All Other Telecommunications" firms potentially affected by our action can be considered small.

2. Internet Service Providers

72. *Internet Service Providers (Broadband)*. Broadband Internet service providers include wired (e.g., cable, DSL) and VoIP service providers using their own operated wired telecommunications infrastructure fall in the category of Wired Telecommunication Carriers. Wired Telecommunications Carriers are comprised of establishments primarily engaged in operating and/or providing access to transmission facilities and infrastructure that they own

and/or lease for the transmission of voice, data, text, sound, and video using wired telecommunications networks. Transmission facilities may be based on a single technology or a combination of technologies. The SBA size standard for this category classifies a business as small if it has 1,500 or fewer employees. U.S. Census Bureau data for 2012 show that there were 3,117 firms that operated that year. Of this total, 3,083 operated with fewer than 1,000 employees. Consequently, under this size standard the majority of firms in this industry can be considered small.

D. Description of Projected Reporting, Recordkeeping, and Other Compliance Requirements for Small Entities

73. In this NPRM, we propose to prohibit wireless carriers from effectuating a SIM swap unless the carrier uses a secure method of authenticating its customer. We also propose to amend our CPNI rules to require wireless carriers to develop procedures for responding to failed authentication attempts and to notify customers immediately of any requests for SIM changes. We also seek comment on whether we should impose customer service, training, and transparency requirements specifically focused on preventing SIM swap fraud. We likewise propose to amend our number porting rules to combat port-out fraud while continuing to encourage robust competition through efficient number porting. Specifically, the Commission also proposes to amend the LNP rules to require carriers to send customers a text message or push notification whenever a porting request is made; to require carriers to allow customers the option to freeze their accounts to prevent any unauthorized port-out requests; and to codify the data fields wireless carriers must use to validate a port request. Finally, we also seek comment whether we should adopt any other changes to our rules to address SIM swap and port-out fraud, including the difficulties encountered by victims of these schemes.

74. Should the Commission decide to modify existing rules or adopt new rules to protect customers from SIM swap or porting-out fraud, such action could potentially result in increased, reduced, or otherwise modified recordkeeping, reporting, or other compliance

requirements for affected providers of service. We seek comment on the effect of any proposals on small entities. Entities, especially small businesses, are encouraged to quantify the costs and benefits of any reporting, recordkeeping, or compliance requirement that may be established in this proceeding.

E. Steps Taken to Minimize the Significant Economic Impact on Small Entities, and Significant Alternatives Considered

75. The RFA requires an agency to describe any significant, specifically small business, alternatives that it has considered in reaching its proposed approach, which may include the following four alternatives (among others): "(1) the establishment of differing compliance or reporting requirements or timetables that take into account the resources available to small entities; (2) the clarification, consolidation, or simplification of compliance and reporting requirements under the rule for such small entities; (3) the use of performance rather than design standards; and (4) an exemption from coverage of the rule, or any part thereof, for such small entities."

76. In this NPRM, we seek comment whether the Commission should modify its CPNI or LNP rules to protect customers from SIM swap and port-out fraud, and, if so, whether our proposals would be effective to do so. In this NPRM, we seek comment on the impact that any proposed rules could have on smaller carriers. We also seek comment on the benefits and burdens, especially the burdens on small entities, of adopting any new or revised rules regarding the customer authentication and porting process. Specifically, we seek comment whether the proposed requirements would impose additional burdens on smaller carriers; whether smaller carriers would face different costs than larger carriers in implementing the new requirements, if adopted; whether smaller carriers would need more time to comply with any new or modified authentication or port-out rules; and whether smaller providers face other obstacles that we have not considered here. The Commission expects to consider the economic impact on small entities,

as identified in comments filed in response to the NPRM, in reaching its final conclusions and taking action in this proceeding.

F. Federal Rules that May Duplicate, Overlap, or Conflict with the Proposed Rules

77. None.

III. PROCEDURAL MATTERS

78. *Ex Parte Rules*. This proceeding shall be treated as a "permit-but-disclose" proceeding in accordance with the Commission's *ex parte* rules. Persons making *ex parte* presentations must file a copy of any written presentation or a memorandum summarizing any oral presentation within two business days after the presentation (unless a different deadline applicable to the Sunshine period applies). Persons making oral *ex parte* presentations are reminded that memoranda summarizing the presentation must (1) list all persons attending or otherwise participating in the meeting at which the *ex parte* presentation was made, and (2) summarize all data presented and arguments made during the presentation. If the presentation consisted in whole or in part of the presentation of data or arguments already reflected in the presenter's written comments, memoranda or other filings in the proceeding, the presenter may provide citations to such data or arguments in his or her prior comments, memoranda, or other filings (specifying the relevant page and/or paragraph numbers where such data or arguments can be found) in lieu of summarizing them in the memorandum. Documents shown or given to Commission staff during *ex parte* meetings are deemed to be written *ex parte* presentations and must be filed consistent with Rule 1.1206(b). In proceedings governed by Rule 1.49(f) or for which the Commission has made available a method of electronic filing, written *ex parte* presentations and memoranda summarizing oral *ex parte* presentations, and all attachments thereto, must be filed through the electronic comment filing system available for that proceeding, and must be filed in their native format (*e.g.*, .doc, .xml, .ppt, searchable .pdf). Participants in this proceeding should familiarize themselves with the Commission's *ex parte* rules.

79. *Initial Regulatory Flexibility Analysis*. Pursuant to the Regulatory Flexibility Act (RFA), the Commission has prepared an Initial Regulatory Flexibility Analysis (IRFA) of the possible significant economic impact on small entities of the policies and actions considered in this *NPRM*. Written public comments are requested on this IRFA. Comments must be identified as responses to the IRFA and must be filed by the deadlines for comments on the *NPRM*. The Commission's Consumer and Governmental Affairs Bureau, Reference Information Center, will send a copy of the *NPRM*, including the IRFA, to the Chief Counsel for Advocacy of the Small Business Administration.

80. *Paperwork Reduction Act of 1995 Analysis.* This document contains proposed new or modified information collection requirements. The Commission, as part of its continuing effort to reduce paperwork burdens, invites the general public and the Office of Management and Budget (OMB) to comment on the information collection requirements contained in this document, as required by the Paperwork Reduction Act of 1995, Public Law 104-13. In addition, pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107-198, we seek specific comment on how we might further reduce the information collection burden for small business concerns with fewer than 25 employees.

IV. ORDERING CLAUSES

81. Accordingly, IT IS ORDERED that, pursuant to the authority contained in sections 1, 4, 201, 222, 251, 303(r), and 332 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 151, 154, 201, 222, 251, 303(r), and 332, this Notice of Proposed Rulemaking in WC Docket No. 21-341 IS ADOPTED.

82. IT IS FURTHER ORDERED that the Commission's Consumer and Governmental Affairs Bureau, Reference Information Center, SHALL SEND a copy of this

Notice of Proposed Rulemaking, including the Initial Regulatory Flexibility Analysis, to the Chief Counsel for Advocacy of the Small Business Administration.

List of Subjects in 47 CFR parts 52 and 64

Communications, Communications common carrier, Individuals with disabilities, Reporting and recordkeeping requirements, Telecommunications, Telephone.

FEDERAL COMMUNICATIONS COMMISSION

Marlene Dortch,

Secretary.

Proposed Rules

For the reasons discussed in the preamble, the Federal Communications Commission proposes to amend 47 CFR parts 52 and 64 as follows:

PART 52 – NUMBERING

1. The authority citation for part 52 continues to read as follows:

AUTHORITY: 47 U.S.C. 151, 152, 153, 154, 155, 201-205, 207-209, 218, 225-227, 251-252, 271, 303, 332, unless otherwise noted.

2. Add § 52.37 to subpart C to read as follows:

§ 52.37 Number Portability Requirements for Wireless Providers.

(a) A wireless provider, including a reseller of wireless service, may only require the data described in paragraphs (b) and (c) of this section to accomplish a simple wireless-to-wireless port order request from an end user customer's new wireless provider.

(b) *Required standard data fields.*

(1) Ported telephone number;

(2) Account number;

(3) Zip code;

(c) *Optional standard data field.* A Passcode field shall be optional unless the passcode has been requested and assigned by the end user, in which case it is required.

(d) *Notification required after port request*. A wireless provider, including a reseller of wireless service, shall notify an end user customer that a port request has been received for the customer's account before executing a simple wireless-to-wireless port request. A wireless provider shall provide this notification to the end-user customer via text message to the telephone number of record for the customer's account or via push notification.

(e) *Account freezes.* A wireless provider, including a reseller of wireless service, shall offer customers the option to lock their accounts to prohibit unauthorized port requests. If the

customer chooses to lock the customer's account, the wireless provider shall not fulfill a simple wireless-to-wireless port order request until the customer deactivates the lock on the account.

PART 64 – MISCELLANEOUS RULES RELATING TO COMMON CARRIERS

3. The authority citation for part 64 continues to read as follows:

AUTHORITY: 47 U.S.C. 151, 152, 154, 201, 202, 217, 218, 220, 222, 225, 226, 227, 227b, 228, 251(a), 251(e), 254(k), 262, 276, 403(b)(2)(B), (c), 616, 620, 1401-1473, unless otherwise noted; Pub. L. 115-141, Div. P, sec. 503, 132 Stat. 348, 1091.

4. Amend § 64.2010 by:

a. Revising paragraphs (b) and (c),
b. Redesignating paragraphs (e) through (g) as paragraphs (g) through (i),
c. Revising newly redesignated paragraphs (g) and (h), and
d. Adding new paragraphs (e) and (f).

The revisions and addition read as follows:

§ 64.2010 Safeguards on the disclosure of customer proprietary network information.

* * * * *

(b) *Telephone access to CPNI.* Telecommunications carriers may only disclose call detail information over the telephone, based on customer-initiated telephone contact, if the customer first provides the carrier with a password, as described in paragraph (g) of this section, that is not prompted by the carrier asking for readily available biographical information or account information. If the customer does not provide a password, the telecommunications carrier may only disclose call detail information by sending it to the customer's address of record, or by calling the customer at the telephone number of record. If the customer is able to provide call detail information to the telecommunications carrier during a customer-initiated call without the telecommunications carrier's assistance, then the telecommunications carrier is permitted to discuss the call detail information provided by the customer.

(c) *Online access to CPNI.* A telecommunications carrier must authenticate a customer without the use of readily available biographical information, account information, recent payment information, or call detail information, prior to allowing the customer online access to CPNI related to a telecommunications service account. Once authenticated, the customer may only obtain online access to CPNI related to a telecommunications service account through a password, as described in paragraph (g) of this section, that is not prompted by the carrier asking for readily available biographical information, account information, recent payment information, or call detail information.

* * * * *

(e) *Subscriber Identity Module (SIM) changes.* Telecommunications carriers shall not effectuate a SIM change unless the carrier uses a secure method of authenticating its customer. For purposes of this paragraph, the following shall be considered secure methods of authenticating a customer: (1) use of a pre-established password; (2) a one-time passcode sent via text message to the account phone number or a pre-registered backup number; (3) a one-time passcode sent via e-mail to the e-mail address associated with the account; or (4) a one-time passcode sent using a voice call to the account phone number or a pre-registered backup number. These methods shall not be considered exhaustive and an alternative customer authentication measure used by a carrier must be a secure method of authentication. For purposes of this section, SIM means a physical or virtual card contained with a device that stores unique information that can be identified to a specific mobile network.

(f) *Procedures for failed authentication for SIM changes*. Wireless carriers shall develop, maintain, and implement procedures for responding to multiple failed authentication attempts.

(g) *Establishment of a password and back-up authentication methods for lost or forgotten passwords.* To establish a password, a telecommunications carrier must authenticate the customer without the use of readily available biographical information, account information, recent payment information, or call detail information. Telecommunications carriers may create

a back-up customer authentication method in the event of a lost or forgotten password, but such back-up customer authentication method may not prompt the customer for readily available biographical information, account information, recent payment information, or call detail information. If a customer cannot provide the correct password or the correct response for the back-up customer authentication method, the customer must establish a new password as described in this paragraph.

(h) *Notification of account changes.* Telecommunications carriers must notify customers immediately whenever a password, customer response to a back-up means of authentication for lost or forgotten passwords, online account, or address of record is created or changed. This notification is not required when the customer initiates service, including the selection of a password at service initiation. This notification may be through a carrier-originated voicemail or text message to the telephone number of record, or by mail to the address of record, and must not reveal the changed information or be sent to the new account information. Telecommunications carriers shall notify customers immediately of any requests for SIM changes through means that effectively alert customers in a timely manner.

(i) *Business customer exemption.* Telecommunications carriers may bind themselves contractually to authentication regimes other than those described in this section for services they provide to their business customers that have both a dedicated account representative and a contract that specifically addresses the carriers' protection of CPNI.

[FR Doc. 2021-22099 Filed: 10/14/2021 8:45 am; Publication Date: 10/15/2021]